International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

BLACK HOLE DETECTION USING COUNTERS AND TIMERS IN MANET

Muzamil Yahya[1], Rajeshekhar C Biradar[2]

[1,2]Department of Electronics and Communication Engineering

REVA University Kattigenhalli, Bangalore, India

ABSTRACT

Mobile Ad-hoc Networks(MANETs) is one of the successful groups of wireless mobile nodes that communicate with available bandwidth and limited power and offers unhampered mobility without depending upon un-divulged infrastructure.MANETs provide sporadic connectivity and adapt to changes very rapidly. MANETs are decentralized networks, where network organization and massage delivery is executed by mobile nodes themselves i.e., each and every node acts like both client as well as server. MANETs have become an agitative and cardinal technology in recent years because of self-configuring nature and are used in various applications, such as battle field, vocation applications, faraway areas, military applications, emergency communications, mobile conferencing and in disaster conditions. The nodes in MANETs are truss or lash to each other by end to end networks.

Due to its nodal mobility and unpredictably changing topology, lack of infrastructure and no central management system, it is more venerable to attacks than their counterpart networks. MANETs are procumbent to variety of attacks enormously in their avenue side. One of the major security problems in MANETs is called black hole problem. It occurs when a malicious node referred as black hole node attracts data packets and drops them instead of forwarding by consigning the fake reply for route request. This malicious node conducts its mischievous behaviour during process of route discovery and has impact on both routing and delivery ratio of packets black hole attack is a kind of fabrication attack which degrades the QOS in terms of packet dropping. In this paper we propound a discernment system which includes counters and timers and adding trust values of nodes in routing protocols to detect the black hole nodes in MANETs with reduced routing, storage and computational overhead. The proposed detection algorithm which uses timers and counters to sight the black hole node in network has detection efficiency of more than 80% and in some cases reaches upto 98%. The silent feature of this technique is its lucidity, less overhead and productiveness in perceiving vengeful nodes.

Keywords*: MANETs,AODV,Trust,Black hole nodes,Security attacks,NS2*

I. INTRODUCTION

A MANETs is self- configuring, self-managed, infrastructure less network of ambulant nodes fetter via by wireless links, mingling of which forms a spirited topology. Nodes can easily annex or leave the network at any extant of time. Owing to nodal mobility, the network topology changes speedily and incalculably over time and time. Each node acts both host as well as router to route packets in the network. Nodes amalgamate with each other to route the control packets and the data.

Nodes in MANET are collectively responsible for network management and they changes configuration according to their needs. Every mote helps all other motes in the network for flowing the information about the contemporary configuration. Due to lack of aforementioned network infra-structure or amalgamate administration these networks can be frame worked at any time and place. MANETs have a variety of applications ranging from military application; emancipate areas such as connecting soldiers on the battle field, emergency operation, campus networks, and vehicular communication to emergency preparedness telecommunication such as communication at disaster sites due to earth quake or flood. MANETs are useful due to less infrastructure, easy installation, low cost bandwidth and low power consumption. Besides this application and advantages MANETs are still not perfect. To underpin connectivity, nodes use some routing protocols such as AODV,DSR and DSDV.

As we know in MANETs nodes are mobile and have lack of infrastructure, dynamically changing topology that makes them prone to scads of attacks. One of these blitzes is black hole attack.

Black hole attack is active and Denial of Service attack in which attacker uses the routing protocol especially AODV to announce itself having unrivalled route to the node whose packets it wants to drop or modify. This type of attack significantly demeans the network performance, such as packet delivery rate and throughput, because of their redone packet drop and the routing load due to frequent route reconstruction.

AODV one of the basic and overriding reactive protocol used in MANETs is significantly browbeat by black hole because a black hole node can easily make the source fool by claiming diminutive and natural route to terminus mote and attracts data packets and relinquish or revamp them instead of redirecting to correct node. By transmitting imprecise information about routing to the fatality nodes, this blitz is generated in the nodes of routing table to give rise to deceptive route entries.

There are two types of black hole attacks:

a) Single or Solitary black hole attacks: In this type of black hole blitz only one malicious node sends hoax reply with an apparently valid route to destination and drop packet instead of forwarding.

b) Co-operative or Collaborative black hole attacks: In this type of blitz's number of malicious nodes attack on the route and gain the route between source and destination and hence complete atrophy in throughput and increase in packet drop ratio in the network. The black hole nodes in a network may perform various noxious effects that are given as:

- Acts as a source node by deny the route request packet
- Acts as destination node by misquote the route reply packet.
- Increasing sequence number and decreasing the hop count, when boosting route request packet

II. AODV

AODV is one of the basic widely used reactive routing protocols in MANET. It allows the mobile nodes to proceed massages through theirneighbours to the nodes with which they cannot directly communicate. AODV inaugurate a route between source and destination nodes when it is craved by the source node that is why called on demand routing protocol. AODV wields control packets route request(RREQ) and route reply (RREQ) for

route inauguration.AODV makes sure that this route does not contain loops and tries to find the shortest path possible.

The route discovery process in AODV is as follows and is shown in figure1:

- Source Sbroadcasts an RREQ packet's to their neighbour nodes 1 and 2.
- The neighbours 1 and 2in turn broadcast the packet to their neighbours 3 and 4 until the packet outstretchto intermediate node that has neoteric route information about the destination node or until the packet reaches the destination.
- Node discards an RREQ packet that is already seen.
- If the node that received the RREQ packet is destination node or an intermediate node that has a fresh enough entry for the destination in its routing table, the destination/intermediate node responds by unicasting a RREP packet back to the source node.
- The RREP packet is routed back to source node along the reverse path that is setup when RREQ packet is forwarded.

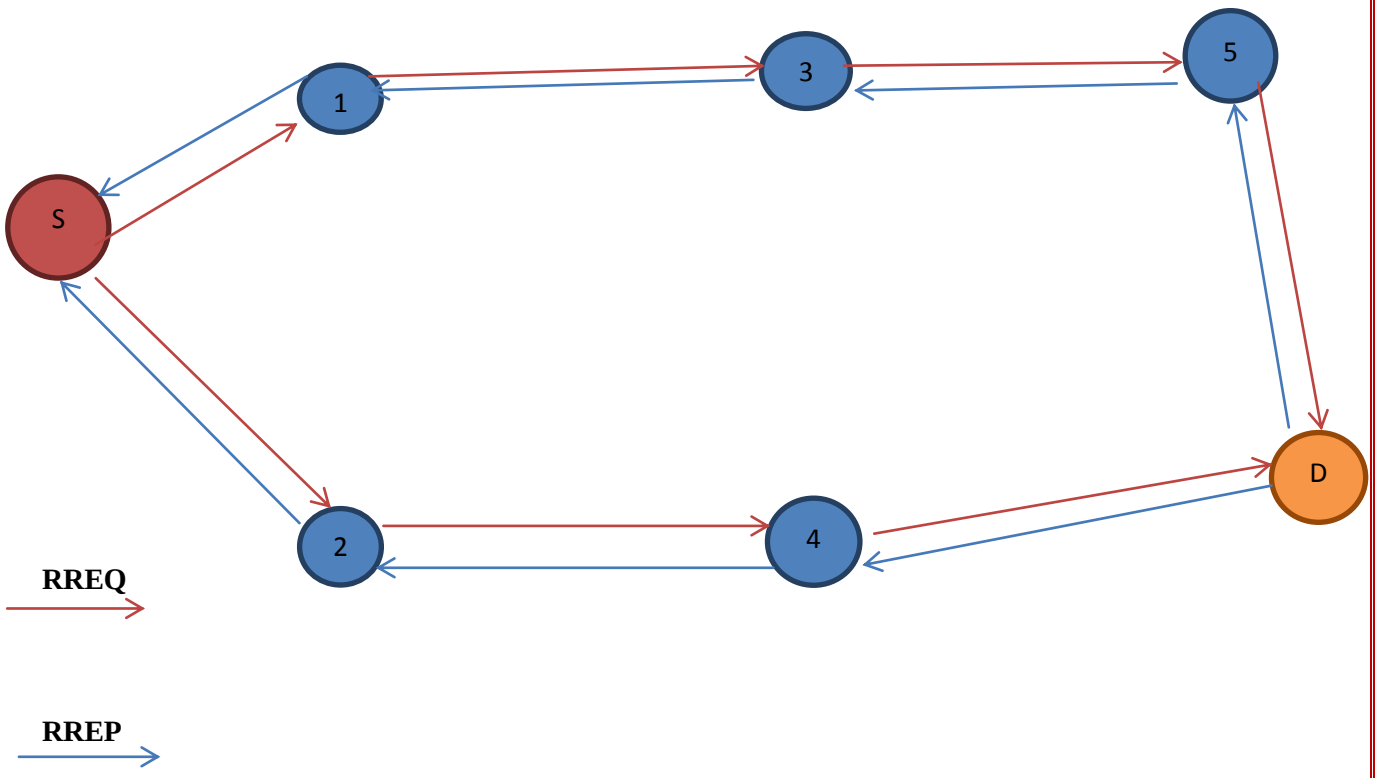

Fig 1: Route Discovery in AODV

Packet format of RREQ and RREP is delineated in figure 2 and figure 3

Type	J	R	G	D	U	Bashful	Hop Count
RREQ ID							
Terminus IP Address							
Terminus Sequence Number							
Initiator IP Address							
Initiator Sequence Number							

Fig 2: RREQ format

Type	R	A	Bashful	Prefix Size	Hop Count
Terminus IP Address					
Terminus Sequence Number					
Initiator IP Address					
Initiator Sequence Number					
Lifespan					

Fig 3: RREP format

The field in the presentation are briefly explained as:

'Type'defines packet type 1 for RREQ and 0 for RREP .The Join flag and Repair flags are reserved for multicast, 'G' flag indicates whether a undue RREP should be unicast to the node specified in the terminus IP address field, 'D' flag indicates destination only flag and is set when only the destination responds not intermediate node and last U flag indicates Unknown flag and is set when terminus sequence number is unknown. Bashful field is set to zero and Hop Count is number of hops from source to current node in the route and initially set to zero.

RREQ ID indicates sequence number uniquely identifying the particular RREQ and the other fields are Terminus IP address is address of destination and sequence number is last known sequence number of the node the initiator IP address is address of originator node and sequence number is current sequence number of the of the initiator node.

Similarly the field in RREP packet has their meaning and are defined as:

Type field is 0 for RREP packet and Flags 'R' is reserved for multicast and 'A' flag for Acknowledgment required. The field Prefix size is set to zero or indicates that it is possible to use the identical avenue for other addresses that begin with same bits as the address in Terminus.

The lifespan field indicate the amount of time that each RREP should be appraising as valid by the receiving node.

The black hole attack is delineated in figure 4 where S denotes Source node and M denotes malicious node and nodes 1,2 and 3 denotes neighbour and intermediate nodes respectively and node D denotes Terminus node .

When Node S wants to send data to node D before this it sends control packet RREQ and receives RREP packet for route establishment and starts sending data .In normal condition packets are correctly forwarded and received but when this malicious node enters into network whole scenario changes and this node sends fake

reply packets to source S and attracts all packets which source wants to send his intended Terminus node .This results in degradation in network performance.

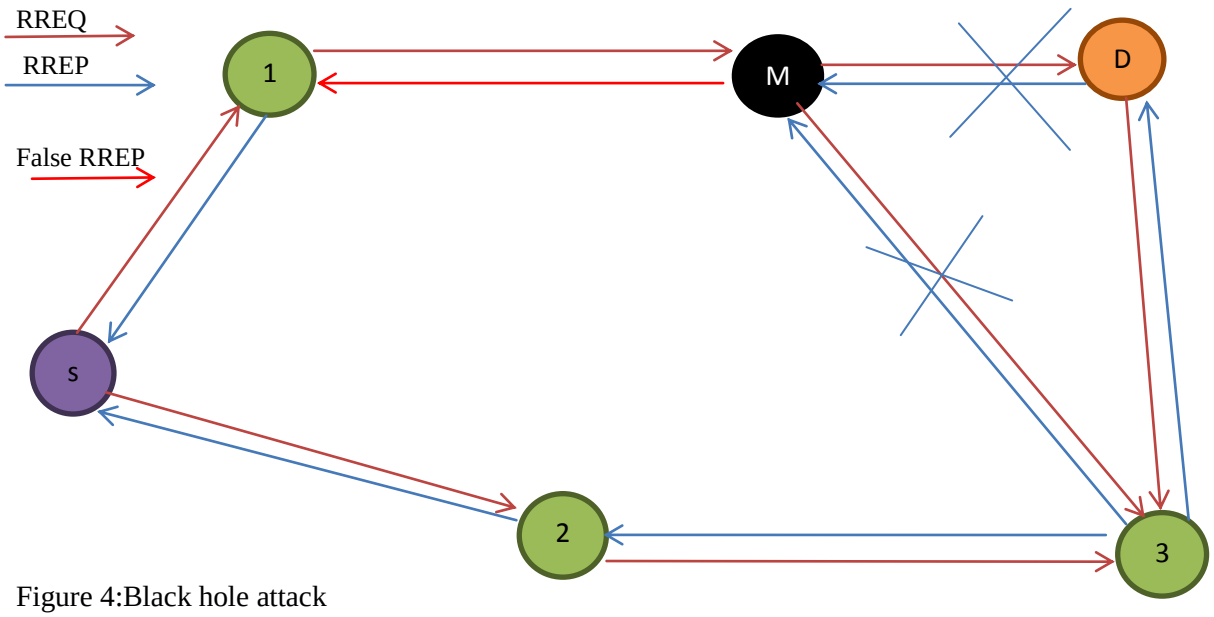

Figure 4:Black hole attack

As shown in fig 4 as Source broadcast RREQ using broadcast IP address 255.255.255.255 all nodes receive RREQ packet which are in transmission range of source node S and they forward this control packet their neighbours and they forward to their neighbours and so on until it reaches to its incipient destination node. Due to node mobility and changing topology it is easy for attackers to put their malicious node to the network to snatch all useful data. There are various attacks inMANETs which degrades the performance of network .One of these attack iscalled Black hole attack. This is Data Traffic attack in which nodes send fake reply to source node claiming that it has shortest route to reach destination. As shown in figure4 node S broadcasts RREQ packet and the malicious node M responds it quickly than others valid nodes. It is similar to black hole in universe that attracts all physical quantities like matter and energy which passes through it and disappears.In similar way black hole drops all packets that are passed through it. As in figure node M sends fake RREP packets to source with highest sequence number and less hop- count. The source node S thinks that it is correct node and update this entity in its routing table and use it in future also that is really a matter of concern because every time when source sends data it just drops it, hence reduces the packet delivery ratio and throughput of network. This is why it is necessary to eliminate this attack from network.

III. RELATED WORK

There are many solutions proposed for black hole detection and focused on developing efficient mechanism to secure the routing in MANETs. Various secure routing, intrusion detection and response mechanism have been proposed. But nearly a few among them detect black holes. Reviews of some strategies are briefly discussed below.Sergio Mart[2] discusses two tools watchdog and path-raterfor detecting and mitigating routing misbehaviour. Watchdog promiscuously listens to the transmission of the next node in the path to detect misbehaviours. Path- rater keeps the rating for other nodes ranges vary from 0 to 0.8 where 0.5 signifiesnode as neutral. Watchdog is used todetect and identify the malicious node, while path- rater performs the job of isolating that malicious node from the network, but this mechanism has disadvantage that it increases memory overhead in the network. Buchegger and Boudec [5] proposed Protocol Corporation of nodes fairness in dynamic ad-hoc network (CONFIDENT). This protocol adds trust manager and reputation system to watchdog and path- rater scheme. The trust manager evaluates the events reported by watchdog and sends alarm to neighbour regarding malicious node. Neelam [6] proposed mechanism for avoiding black hole attacks by assigning unique ID number to all the normal nodes exist within AOVD and transfer data only via these nodes. Zhang, Lee and Herang proposed intrusion detection (ID) and response system[4,9], each node in this scheme is responsible for detecting signs of intrusion locally and independently but neighbouring nodes can collaboratively investigate in a border range. Individual IDs agents are placed in each and every node.

IV. PROPOSED APPROACH

In this section of paper we propose an algorithm for detection of black hole nodes in MANETs. This black hole node is a malicious node which instead of forwarding the data to other nodes it either modifies or drops the packet. While developing the algorithm we have taken some assumptions:

- Malicious node does not acknowledge with data packet in the network.
- Black hole node will receive the packet but instead of forwarding it, it either modifies it or drops the packet to lower the packet delivery ratio and network efficiency.

V.PROPOSED ALGORITHM

We are making an approach to perceive and diminish the effects of blackhole attack in AODV routing protocol. In this approach, in order to discern black hole attack, counters and timers are taken into account. Since we know in AODV routing protocol control packets (RREQ AND RREP) are used for route establishment. Once a route has been entrenched the data packet has to forward via this established path. Eachnode in the network is having timers and counters. This activity of a node in the network shows its honesty to forward the packets. In order to participate in data transfer process, nodes must demonstrate its honesty.

Here is brief description of counters and timers:

Drop Counter: This is counter which is updated at two places:

- When a packet is received by the node from its neighbour.
- When the node forwards it correctly to other node in the network. This counter is incremented by one for each incoming RREQ packet and is decremented by one for each outing RREQ packet.

Sense Timer: This timer is used as detection period for mobile nodes to identify whether a node correctly forwards the received RREQ packet during this period or not. If it dispatches it correctly the counter is decreased by one otherwise incremented by one.

Reward Timer: Since we know the source node broadcast RREQ packet, so sometimes nodes received duplicate RREQ. The timer award some time to node to drop this duplicate RREQ without penalized. Is This Timer is started only when a legit RREQ is dispatched during this discernment period.

The brief description of Algorithm is as follows:

At first the originator node broadcast the RREQ packet to their neighbours, because of broadcast nature of RREQ some nodes receive duplicate RREQ and this node checks if this is twofoldRREQ and reward timer is imminent that means it gives time to node drop this duplicate RREQ without penalize the node and a message "Not a newentreaty " is displayed and the node checks if this intermediate node is destination node then send RREP packet with neighbour list otherwise increment the drop counter by one.Now, if the RREQ is fresh then we initialize both Sense Timer and Reward Timer to their present value i.e., time in the system clock and start the Sense Timer.

The Sense Timer shows reading of present time plus sense time and we check what is the value in the timer is and depending upon it we increment the value of drop counter. Now, when node starts to send RREQ packets we calculate the time to send for this packet i.e., total time taken by node to forward the packets and compares the value to value of Sense Time . If the value of Time To Send is greater than Sense Timer then Drop counter is incremented otherwise start the Reward Timer and observe value of it and decrement the counter after all steps compare the value of the Drop Counter to a predetermined Threshold Value .If the value of Drop Counter is greater is greater than Threshold Value than mark the node as Black hole node and stop the process.

The above steps are discussed in the programme given below:

Algorithm:

Notations

SR-N - Source node

DS-S - Destination node

RREQ - Route Request

RREP - Route Reply

N-N - Neighbour node

IN-N - Intermediate node

Present Time - PT

Drop-Counter -DC

Sense –Time -ST

Reward Time - RT

Time – To – Send -TTS

Threshold –Value - TV

Input: A RREQ to neighbour nodes

Output: Detection Status of node for all RREQs to this node does

BEGIN

1. SR-N broadcast RREQ
2. Each in-n gets the RREQ from its N-N and checks

   if request is duplicate RREQ**then**

   *is duplicate RREQ =T*rue and RTisforthcoming

   Then

   message "**Not a New Entreaty**" and caper all the next steps and checks

   if DS-S = IN-N

   sendRREP with neighbour list

   else

   DC= DC+ 1

   end if
3. **if** RREQ is Fresh

   then

   ST= PT

   RT=PT
4. Start the ST such that

   ST=PT+ ST

   DC=DC+1
5. Calculate TTS for this packet

   ifTTS>ST

   then

   DC=DC+ 1

   else

   Start the RT such that

   RT= PT+ RT

   DC= DC– 1

   ifDC>TV

   then

   "**Label the node as Black hole**" and send alarm to network and conclude

   end if

end for

END

V. MATHEMATICAL PERUSAL

In this portion of paper we proffer a mathematical model which calculates the trust experienced by nodes in successful and unsuccessful transmissions. Trust value of current node depends upon past behaviour of other node in the same transmission range, same as humans which trust only those people which are trustworthy in past. Trust is calculated depending upon ability to forward packets and RREQ.

Suppose X and Y denotes number of successful and unsuccessful transmissions in the network.

If X > Y then

$$T_{exp} = 1 - \frac{1}{\left\{\left(\frac{2X-Y}{X+Y}\right)\times Ws\right\}+2} \quad (1)$$

Where Ws denotes the weight of successful transmission and is chosen on how many transmissions takes place. The equation suggests that trust experienced by node in successful transmission is in the range of 0.5 to 1 by putting appropriate values of given terms.

e.g., if X=3, Y=2 on putting in equation (1), we get 0.568 and hence above 0.5 and therefore nodes are trustworthy.

Now, if Y>X then

$$T_{exp} = 1 - \frac{1}{\left\{\left(\frac{2Y-X}{Y+X}\right)\times \frac{1}{Wu}\right\}+2} (2)$$

Where Wu denotes weight of unsuccessful transmissions and this equation suggests that the trust value experienced by nodes during unsuccessful transmission is less than 0.5 by putting appropriate values of given terms in above equation.

e.g., let Y=4,X= 1 and Wu=0.8 and put these values in equation (2) we get value of 0.42 which implies that nodes are untrusted.

The trust value of node Y is computed based on advice of node X as discussed above and is delineated by the equation:

$$T_Y = \frac{\sum_{l\neq X} T_X^l}{\sum_{l\neq X} T_X^l} + \frac{\sum_{l\neq Y} T_X^l * T_l^Y}{\sum_{l\neq Y} T_X^l} (3)$$

Where '*l*' is evaluated node whose value is evaluated from node X , T_X^l is trust of node '*l*' given by node X and T_l^Y is trust value of node Y given by node '*l*' whose value is calculated from past node X as we know the values of all nodes depend on each other . The trust value computed by node X for node Y in the current time is given by the equation:

$$T_C = W_1 T_{exp} + W_2 T_Y \quad (4)$$

Where W_1 is fraction of number of packets remit from a node in successful transmission to the number of packets gathered by that node. Higher value of W_1 may be 1 that means all packetsare correctly remit and there is no packet drop. While as W_2 is ratio of number of RREQ packet gather to the number of RREP remit.

Where $\mathbf{W_1 + W_2} = 1$

The trust values are continuous values in the ambit of [0 1] with representation that if values are less than 0.5 indicates untrusted or malicious nodes, values of trust is 0.5 that means neutral node and values above 0.5 to 1 and are considered as trusted nodes and RREP packet are accepted from only those nodes not the malicious ones.

VI. RESULTS

The whole scenario has been implemented on NS2 simulator.Simulation parameters we used in implementing this algorithm are shown in table as**:**

TABLE 1: Simulation Parameters

S. No.	Simulation Parameters	Values
1	Simulator used	Network Simulator(2.34)
2	Number of Nodes	35
3	Number of Vitriolic nodes	2
4	Subjugate Protocol	AODV
5	Area Size	1000 × 1000m
6	MAC	802.11
7	Traffic Source	CBR
8	Propagation Model	Two Ray Model

9	Antenna	Omni-directional
10	Speed	20m/sec
11	Pause Time	1 sec

The result we get after simulation of this algorithm is shown in various figures below:

We examine networks for both with these vitriolic nodes and without vitriolic nodes and we see results from various graphs below:

1) Graph of Throughput which shows the throughput is much higher in normal networks as compared to networks which contain vitriolic nodes.
2) Graph of PDR which indicates that Packet delivery ratio is much higher in networks without malicious nodes as compared to vitriolic networks and is better from previous techniques.
3) Graph of Overhead: From previous techniques we see overhead is eliminate to less extent but with this technique we are successful to eliminate the overhead from network to very large extent.

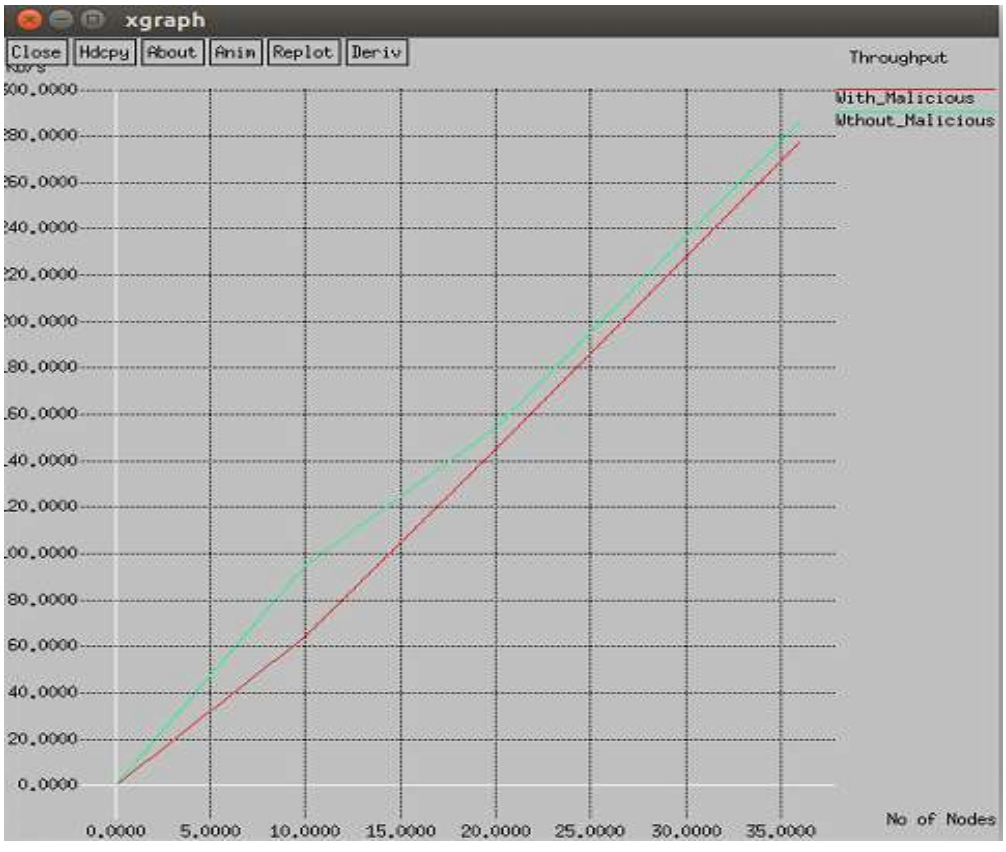

Fig 5: Throughput Graph

In this figure, it is shown that graph of Throughput and throughput is more than in network which does not contain malicious nodes than networks which contain malicious nodes. It is necessary to removes these nodes from network to achieve high performance of network.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

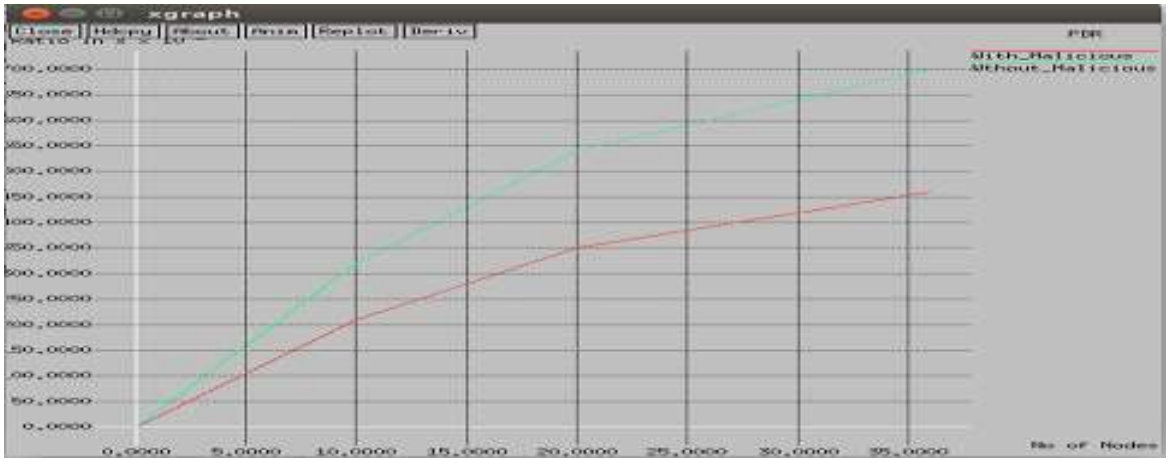

Fig 5.1: Packet Delivery Ratio

Figure 5.1 shows Packet delivery ratio graph with valid nodes and with malicious nodes. As we seen from figure the packet delivery ratio is much higher in MANET which contain valid nodes . So, it is necessary to detect and removes the malicious nodes from network to achieve high performance network and is less in previous scenarios.

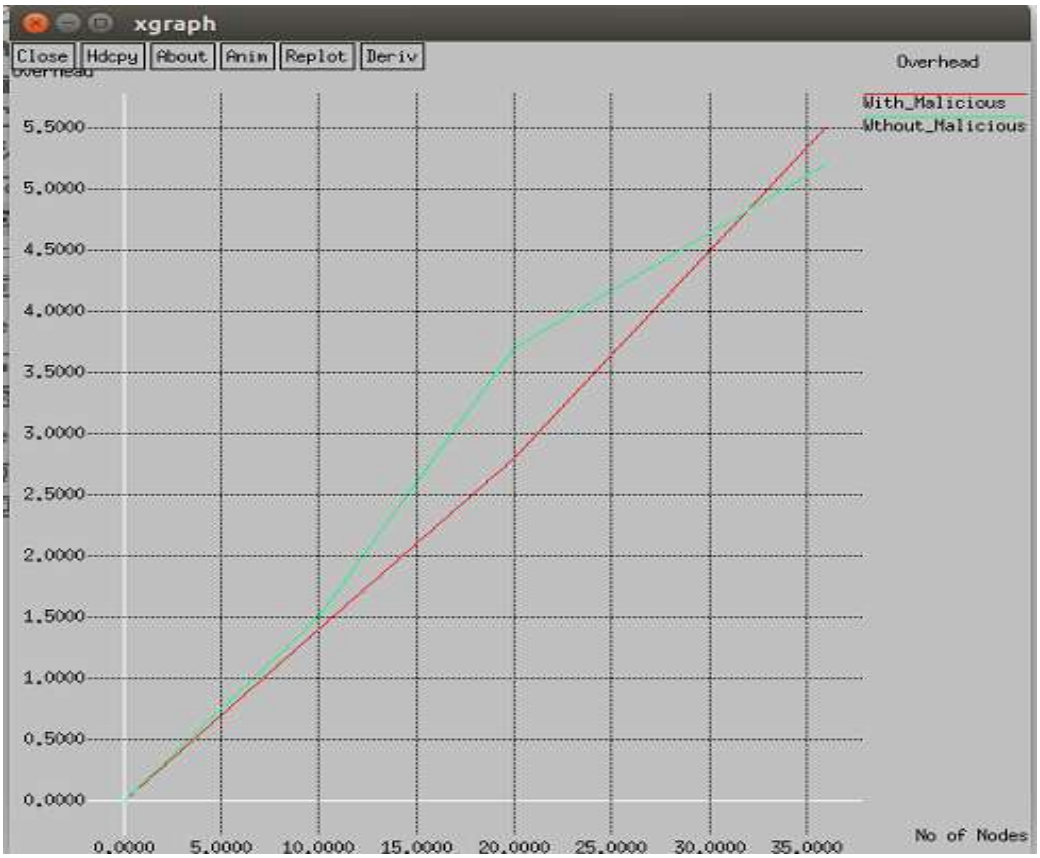

Fig. 5.2 Overhead Graph

Figure 5.2 shows Overhead graph .The overhead is more in networks with malcious nodes as compared to network with normal nodes. The overhead is less in this scenerio as compared with other scenerios.

VI.CONCLUSION

Since we know that nodes in MANETs are mobile, decentralized network, self-configuring network in which nodes acts as both router as well as host . Nodes can nimbly join or vamoose the network without permission because of these facts they are prone to sundry strafes.Black hole is one of the strafe in MANETs and we tries to eliminate these black hole nodes from network. So we give a simple algorithm to solve this problem of black holes .In this approach we use Timers and Counters to discern and migitate the black hole nodes.The solution is been analysed, tested with different parametres such as Throughput ,Packet delivery ratio and overhead. The apprehension efficacy of this approach is more than 85% and in some cases it reaches upto 98%.Thus in general our approach shows very predicting results in detecting these black hole attacks. The distinctive cue of this model is its lucidity, lowcost and efficacy in detecting the baleful nodes.

REFERENCES

[1] Yuvraj Singh , Sanjay Kumar Jena : Intrusion detection systemfor detecting malicious nodes. " ISSN, ISBN" (2011)

[2] Anum, F . , Mouchtaris, P.:Security for wireless Ad Hoc Networks.WILEY , 2ndedn. (2007)

[3] Rajshekhar Tiwari, Manish Sharma :Analysis of trust based and Intrusion based black hole preventation in AODV in MANET

[4] Marti.S , GiuliTj, Laik ,Baker M: Mitigating routing misbehaviour in mobile adhoc network; August 2000.

[5] Khin, Ei , Thandar Phyu. "Comparative analysis of Black hole attack solutions in AODV protocol. "IJCCER 1.2 (2013).

[6] S.Dokurer , Y.M.Erien , C.E.Acar, " Performance analysis of Adhoc networks under black hole attack," in IEEE proceedings Southeast con, 2007.

[7] Tamilselvan l, Sankaranarayanan V, "Preventation of Black hole Attack in MANET", 2nd International Conference in wireless Broadband and Ultra Wideband communication, Sydney, Australia , August 2007.

[8] C.E.Perkin, E.M. Royer, S.R.Das, Mobile Ad Hoc Networking Working Group, Internet Draft, 2003.

[9] Taku Noguchi, Takaya Yamamato, Black Hole Attack Preventation Using Dynamic Threshold in Mobile Ad HOC Networks.2004.